

LEGISLATIVE AUDIT COMMISSION



Review of
Department of State Police
Year Ended June 30, 1999

622 Stratton Office Building
Springfield, Illinois 62706
217/782-7097

REVIEW: 4118
DEPARTMENT OF STATE POLICE
YEAR ENDED JUNE 30, 1999

FINDINGS/RECOMMENDATIONS - 11

ACCEPTED - 9
IMPLEMENTED - 2

REPEATED RECOMMENDATIONS - 4

PRIOR AUDIT FINDINGS/RECOMMENDATIONS - 10

This review summarizes an audit of the Department of State Police for the year ended June 30, 1999, filed with the Legislative Audit Commission March 25, 2000. The auditors conducted a compliance audit in accordance with the Single Audit Act and OMB Circular A-133. The auditors indicated that the financial statements of the Department are fairly presented.

The Department of State Police was established January 1, 1970 and was reorganized by Executive Order in 1977 and again in 1993. The Department's responsibility is to maintain order as mandated by the statutes, while safeguarding the rights and privileges of all citizens of the State. The Department is divided into the Human Resources Command and four divisions: Operations, Forensic Services, Administration, and Internal Investigation. Through its Division of Operations, the Department maintains 21 local headquarters around the State to provide a full range of law enforcement services to the citizenry and law enforcement community.

Mr. Gene Marlin was the Director during the first six months of the audit period. Sam W. Nolen is the Director of the Department currently, and has held that position since January 16, 1999. Mr. Nolen was a State Police officer for 29 years. When he retired from the State Police in 1990, he was the Acting Director.

The following presents the average number of employees by position for the fiscal years ended June 30:

	FY99	FY98
Sworn Officers	1,980	1,908
Civilian Administration	1,375	1,346
Communications	305	291
TOTAL	3,660	3,545

REVIEW: 4118

Between FY98 and FY99, the average number of employees increased by 115. FY99 employment figures mirror FY97 figures exactly. In FY99, the Division of Administration gained 28 positions and the Division of Operations gained 95 positions.

The following table presents a comparison of activities and performance for the fiscal years ended June 30:

	<i>FY99</i>	<i>FY98</i>
Cases Opened	8,781	7,799
Convictions	7,471	6,396
Motorist Assists	122,781	133,611
Vehicle Code Citations	409,262	394,827
Arrests	26,334	25,582
Cases Worked by Crime Laboratories	53,783	53,850
Crime Scene Cases	3,860	3,614
Fingerprints Received/Processed	568,511	611,675
LEADS System Inquiries	132,440,656	126,133,959
Sex Offenders Registered	14,682	10,476
FOID Applications Processed	228,051	200,232

Expenditures From Appropriations

Appendix A presents a summary of expenditures for the year under review and FY98. Appendix B provides a summary of appropriations and expenditures for FY99 and FY98. The General Assembly appropriated a total of \$311,490,000 to the Department in FY99. Expenditures increased from \$273,331,066 in FY98, to \$291,446,024 in FY99, an increase of \$18,114,958, or 6.6%.

Approximately 67% of the Department's appropriations are from the General Revenue Fund, 17% from the Road Fund, and the remaining 16% from other funds. Expenditures from the General Revenue Fund increased from \$183,674,176 in FY98, to \$200,620,345 in FY99, an increase of \$16,946,169, or 9.2%. The increase in expenditures was attributed primarily to the increase in the number of employees. Additionally, the Juvenile Justice Program received \$3.2 million for fingerprint processing. Expenditures for the Chicago Forensic Lab are reported within the detail expenditure object codes in FY99, rather than as a lump sum as in FY98.

Cash Receipts

Appendix C provides a summary of the Department's cash receipts for FY99 and FY98. Total cash receipts decreased slightly \$48,746,024 as of June 30, 1998, to \$48,734,321 as of June 30, 1999. The variation in receipts is due primarily to fewer processed cases of Medicaid fraud and fluctuations in asset forfeiture. Also during FY99, the State Police stopped providing racetrack security on a regular basis, and the fund created in FY98 to provide DNA testing of sex offenders was operational for the full year in FY99.

Accounts Receivable

Appendix D summarizes the accounts receivable of the Department at June 30, 1999 and 1998. Accounts receivable increased from \$1.8 million at June 30, 1998 to \$2.2 million at June 30, 1999. Approximately \$1.4 million receivables were over one year old at the end of FY99.

Property and Equipment

Appendix E summarizes the changes in property and equipment. The beginning balance as of July 1, 1998 was \$195,065,000, and the ending balance was \$204,910,000 as of June 30, 1999, an increase of \$9,836,000, or 5%. Of the ending balance, approximately \$152,700,000 is in equipment and \$45,400,000 in buildings and building improvements, with the remainder in land and capital lease assets.

Accountants' Findings and Recommendations

Condensed below are the 11 findings and recommendations presented in the audit report. There were four repeated recommendations. The following recommendations are classified on the basis of information provided by Gail E. "Bud" Pruett, Chief Fiscal Officer, in email received August 21, 2000.

Accepted

- 1. Institute measures to strengthen project management. Develop policies and procedures, implement a system development methodology, and establish**

appropriate monitoring mechanisms to ensure projects meet standards, maintain and promote system integrity and quality control, efficiently utilize resources, and meet objectives in a timely manner. At a minimum, include the following in systems development methodology and standards:

Accepted - continued

- feasibility studies and cost benefits analysis;**
- approval process for initiating system development activities;**
- appropriate documentation required for each phase of development life cycle including the development of system, operations and user manuals;**
- user training;**
- software and hardware specifications;**
- general and detail design specifications;**
- testing requirements, including requirements for user and programmer testing;**
- project reviews including periodic “milestone” reviews and post-implementation reviews;**
- monitoring techniques to ensure that all contractual conditions have been met and that the system purchased is operational prior to approving final payments; contract procedures that specify project deliverables including system components, source code, documentation, project time frames, and estimated hours; and**
- require project managers to document approval of contract expenditures.**

Ensure compliance with standards and methodology once established, and hold a significant percent of contract amounts until deliverables are completed and/or received. Recoup contract monies for deliverables not received.

Findings: The Department had not established system development standards nor contract monitoring procedures to ensure that computer systems were appropriately managed to efficiently and effectively support the Department. The lack of standards and procedures resulted in systems being developed and paid for that did not adhere to contractual requirements or meet the needs of the Department.

The Department’s system development manual was outdated and did not reflect the current processing environment. Sufficient contract monitoring procedures did not exist to ensure that contractors delivered usable systems that complied with the contractual provisions.

REVIEW: 4118

Auditors reviewed four system development projects and identified project management problems with three of the four:

- One contract was paid in full, \$1.8 million, even though the contractor installed the system at only eight of 22 sites.
- One contract was paid in full, \$175,000, in August 1998 for a system that was not in operation late in 1999.
- One contract was paid although the chain-of-custody evidence system was under development for seven years and had not been fully implemented.

Response: Accepted. A Quality Assurance Section has been established within the Information Services Bureau and an Application Development Project Team has been assigned responsibility for strengthening project management. The team has established standards and adopted methodology used by the State Lottery. A detailed project plan has been prepared.

Recent adoption of Department Contract Compliance Procedures addresses contract standards and payment. These standards are currently being implemented within Information Systems Bureau (ISB) and will be incorporated in bureau processes.

2. Enforce written policies and procedures for LANs, mainframes, and information security. Reduce risk of unauthorized access to Department resources leading to compromised data, privacy breach and possible sabotage by adhering to formal policies and procedures. (Repeated-1992)

Findings: The Department had not established adequate security controls over its \$6.3 million computer systems. The Department had approximately 55 LANs located throughout the State and has not ensured compliance with its written policies and procedures for personal computers, LAN administration and information security. Weaknesses noted include:

- users allowed to log on to more than one workstation simultaneously;
- passwords not required for some users;
- password change intervals were excessive or non-existent
- over 840 user accounts had never been used or not accessed for at least 90 days, including some accounts assigned to individuals no longer employed by the Department; and
- all user accounts were not assigned to a specific individual to ensure auditability and accountability.

No identifiable measures had been taken to ensure accountability of network administration access.

REVIEW: 4118

Weaknesses noted in the Department's mainframe computer systems which processes information 24 hours a day, seven days a week include:

- several software security features had not been appropriately implemented;
- passwords not required for some users; and
- default password had not been changed.

Response: The mainframe password identified in the audit was changed 12/99.

Accepted - continued

Significant progress has been made in regard to reducing the number of inactive user accounts in the client/server and mainframe environments. Systems are routinely monitored and deletions are made as needed. Bindview has been obtained and is being used as a tool to monitor user ids and access.

A Security Project team has been established and all applications are being reviewed in regard to passwords, user ids and automatic time-based log off. The team is identifying how to address the audit recommendations in regard to each system. Action has been taken to correct problems where possible and plans are being developed to address the systems where there are large technological, procedural or operational issues.

Because of technical limitations, the 30-minute automatic time-based log off cannot be implemented. Instead, the use of screen locks set to a maximum of 15 minutes will become policy.

- 3. Update change control procedures to require written management approval before modified programs are placed into production. Additionally, restrict programmers from accessing production programs or data, and make individuals responsible for transferring programs into production independent of programming responsibilities.**

Findings: Documented procedures for changing computer programs, last updated in 1991, did not reflect the current computing environment at ISP, were not used by staff and did not ensure that the integrity of the system was maintained. Other weaknesses noted in the change control process include:

- programmers had access to production programs and data;
- programmers had the authority to make changes to programs and then move the programs to production;
- formal management review and approval of program changes was not required;
- controls and audit trails did not exist to effectively prevent or detect unauthorized changes to production programs;

REVIEW: 4118

- date protection of system libraries had not been implemented; and
- documentation of changes was maintained for only six months.

Response: Accepted. A project plan has been developed: the first phase requiring separation of duties was implemented August 1, 2000, with a plan to discontinue all programmers' access to production by October 1. Formal supervisory approval has been added to the change control process; policy has been updated and implemented. Documentation (electronic database and hard copy) of changes dates back to 1987.

A revised change request process has been finalized which strengthens and centralizes controls.

Date protection has not been implemented because ISB provides update authority to system library through RACF security. In addition, updates to system libraries require routing through the change control process. Prior to RACF, ISB used date protection on system libraries.

4. Enhance physical security policies and embark on a security awareness program for all staff as follows:

- **develop and enforce security policies that require the use of cardkey badges and increase staff awareness of the risks of "tailgating" and leaving card-key controlled doors open or unlocked;**
- **develop a form and maintain written approval for all card-key assignments;**
- **eliminate the issuance of multiple card-keys;**
- **obtain training for the staff responsible for maintaining the card-key system to enable them to properly maintain the system;**
- **Ensure audit trail information is maintained for the card-key system, routinely back up the card-key system data and store the backups off-site;**
- **Limit computer room access to the minimum number of staff needing access; and**
- **Review the security over wiring closets and take appropriate action based on the analysis of the risks and costs.**

Findings: The Armory Building in Springfield is the primary location for the administration of the ISP. It also housed the data center which includes critical and confidential information on crime, fingerprints, firearm owner identification, drug interdiction, sex offenders and evidence. Although the building is equipped with a card-key based access system to control access into and within the facility, the auditors identified numerous security weaknesses including:

- Inappropriate use of the card-key system via "tailgating", and card-key controlled doors being propped open;

REVIEW: 4118

- Five staff were assigned multiple card-keys, and 12 people not in the ISB were assigned card-key badges with access to the computer room;
- Inadequate training in the effective use of the card-key system resulted in no regular backups of system data, improper input of new badge assignment resulted in loss of the history file of badge assignments, and a lack of readily available audit trail information; and
- Inadequate security over wiring closets.

Response: Accepted. A revised security policy will be released by September 1, 2000, covering all areas as recommended in the audit. A revised, updated form for issuing access cards, requiring employees signature and the signature of their Bureau Chief has been distributed to all employees, and all employees are being cautioned on the risks of tailgating. The card-key database has been purged and updated as necessary. Access

Accepted - continued

to the ISP Data Center has been restricted to only those employees requiring it for their job duties. All wiring closets in the Armory have been secured to prevent unauthorized access.

5. Develop an enterprise-wide approach to recovering and restoring computer processing should be addressed in disaster recovery plans. Strengthen disaster recovery capabilities by:

- **developing a prioritized list of the critical applications and the required recovery timeframes for each;**
- **ensuring sufficient capacity is available for processing concurrently all critical mainframe applications;**
- **arranging for alternate processing sites for minicomputer and LAN systems;**
- **performing an annual comprehensive test of the disaster recovery plans. Test should include all critical computing platforms and systems and be adequately documented, and the plan should be continuously modified to eliminate any weaknesses identified during testing;**
- **ensuring the disaster recovery plan is current; and**
- **upgrading the fire protection system for the computer facility and the entire Armory building to provide adequate security against potential loss due to fire damage. (Repeated-1986)**

Findings: ISP had not updated its disaster contingency plan to include provisions for recovering its entire computing environment, nor performed a comprehensive test of its mainframe, minicomputer, or LAN disaster recovery capabilities. The mainframe disaster recovery plan was dated 1995. ISP utilizes approximately \$6.3 million of computer equipment which is configured into various computer systems across several platforms including minicomputers, LAN and mainframe systems.

REVIEW: 4118

ISP's mainframe processes the following systems 24 hours a day, seven days a week: hot files (wanted and missing persons, orders of protections, stolen articles, etc) provided to all police departments in the State; arrest reports; criminal history records; illegal interstate transportation of drugs, weapons, and currency; and the queries for Secretary of State drivers' license and vehicle information. These systems are vital to the safety of sworn officers and local citizens.

The auditors noted that the only disaster contingency procedures tested were associated with the recovery of mainframe backup tapes at the backup site. A recovery site for the minicomputer applications did not exist.

In response to prior audit findings, ISP agreed to upgrade the fire protection system at the Armory, appropriate action had not been taken. ISP had developed disaster recovery plans for three of the five critical applications process on the LANs, for the network operating systems, and for remote access.

Response: A disaster recovery plan was finalized in June 2000, with a walk through of the plan conducted in July. ISP is a pilot agency with CMS for mid-range and mainframe disaster recovery projects partnering with IBM and COMDISCO, a firm specializing in data center backup.

Computers have been identified at ISP facilities in Joliet and Chicago as backup servers for LAN applications, should they be needed for disaster recovery. A Disaster Recovery Coordinator has been appointed to oversee all of these activities.

8. Develop and follow formal written procedures for the monitoring, maintenance and account for accounts receivable balances. (Repeated-1998)

Findings: ISP did not have adequate procedures for monitoring and accounting for accounts receivable balances. The auditors noted the following:

- accounts receivable subsidiary records for the State Police Services Fund were \$34,535 greater than the amount reported in the GAAP Reporting Package;
- not all eligible receivables accounts were submitted to the Comptroller's offset system;
- an outdated report was used to estimate the reserve for uncollectible accounts which resulted in a \$4,000 understatement of the reserve for uncollectible accounts; and
- no formal written procedures for writing-off old uncollectible accounts.

Response: Procedures have been revised requiring review and inputs to the GAAP reporting process. In addition, accounts receivable procedures are being completely reviewed, including collection and referral process.

REVIEW: 4118

Procedures now include formal write-off guidelines. Accounts are being reviewed monthly and a number of accounts have been written off.

9. Comply with Statewide Accounting Management System's (SAMS) procedures and State law to ensure property records are complete and accurate.

Findings: The Department did not comply with certain specific requirements of the SAMS related to property control and did not have adequate procedures to ensure all property transactions were properly reflected on the property records. The Department did not adhere to rules governing the administration of internal controls over fixed asset reporting.

Accepted - concluded

When the auditors visited one district office, personnel were unable to locate four of five items selected from the inventory control listing. Additionally, a car located at the facility was not included in the property control listing maintained at the Office of Finance and Budget. Other deficiencies at other offices included improperly deleting items from the inventory control list and not reconciling the Bureau-wide property control system with the Department-wide property control system.

Response: A Property Control Task Force was appointed to review all audit findings and evaluate all problems identified with property control. As a result, ISP policy has been changed and division heads are made more accountable for their annual inventories. In addition, all property locations now have Asset Tracking Manager Software which provides on-line inquiry, reporting, and transfer capabilities to the property location custodians. Updates to procedure manuals are complete and training is planned for this fall.

10. Pay for hours actually worked within the contract period, review invoices to ensure only charges authorized under the contract are paid and only pay for services performed pursuant to the applicable contract. In addition, develop, implement and periodically monitor management controls designed to ensure the future compliance with applicable purchasing and appropriation rules.

Findings: ISP's Information Service Bureau (ISB) entered into numerous "body shop" contracts for a variety of reasons. These contracts, with consultants pre-approved by CMS, usually specify EDP services for up to a certain number of hours to be completed by a specified date. The auditors noted the following:

- Invoices contained overstated numbers of hours worked. Ten invoices, processed between June 1996 and February 1999, were received from five different

REVIEW: 4118

consultants. One set of time records, overstating the actual time worked, was maintained, and then a second set of time records supported actual time worked. The overstated numbers were reported to give the appearance that all hours worked were used before the contract period ended. The consultants were improperly paid \$27,600.

- Consultants were allowed to present incorrect time sheets by converting travel expenditures, which were not specifically allowed in the contracts, into an equivalent number of work hours to get paid.
- Invoices totaling approximately \$36,000 were processed for 640 hours of EDP services of which the majority was not directly related to the contract requirements.

The State Finance Act requires a certification on behalf of the State agency on every voucher for goods and services. The certification states the goods and services specified were for the purpose of the agency and that the expenditure of such goods or services was authorized and lawfully incurred. The certification also states the services met all the required standards set forth in the purchase agreement or contract to which the voucher related and that the amount shown on the voucher is correct and approved for payment. The Act provides for the discharge of any employee who knowingly and intentionally files a false certification.

Response: Effective July 1, 2000, ISP implemented a contract compliance procedure and appointed a Contract Compliance Officer. The procedure strengthens the oversight process by establishing a separate level of continual review during the life of a contract with specific attention to compliance with all requirements of the contracts and State regulations. In addition, project management has been strengthened with emphases on monitoring time logs and providing additional training to those employees responsible for reviewing payment documents.

11. Pay only for contracted services and pay for such services out of correct fiscal year appropriations. Ensure that all billings and billing dates are accurate.

Findings: ISP's Information Services Bureau (ISB) improperly expended FY99 money for FY98 expenditures. A contractor billed ISP for \$521,000 for services rendered in FY98. However, since the contract was not signed until late in June of 1998, ISP requested the contractor to change deliverable dates and resubmit the work products for re-acceptance by the Department in FY99. In order to receive payment, the contractor resubmitted the invoices and was paid in July 1999.

Response: Effective July 1, 2000, ISP implemented a contract compliance procedure and appointed a Contract Compliance Officer. The procedure strengthens the oversight process by establishing a separate level of continual review during the life of a contract with specific attention to compliance with all requirements of the contracts and State regulations. In addition, project management has been strengthened with emphases on monitoring time

REVIEW: 4118

logs and providing additional training to those employees responsible for reviewing payment documents.

Implemented

6. Identify the need for the helicopter unit and adhere to applicable rules and regulation regarding contracting processes.

Findings: ISP did not adequately develop a plan for the need, implementation, utilization or funding of the helicopter unit program. There was no formal mission statement covering its air operations. ISP did not comply with the Administrative Code when awarding the contract for the lease of helicopters. ISP received two bids in response to its RFP. The winning bid contained an obvious error in price. The bid price was stated as \$1,800 per month and the contract was written for \$18,000 per month. ISP did not retain any documentation that there was a change. ISP personnel stated the decision to provide helicopter service was made by the former administration.

Implemented - concluded

Response: Compliance with all recommendations has been accomplished. The Helicopter Unit has been disbanded and the fixed-wing component of Air Operations Bureau expanded to provide enforcement coverage previously provided by the helicopters. Fiscal and contractual issues are being overseen for strict compliance with State regulations. A Bureau mission statement has been finalized and is displayed in each Bureau location.

7. Develop written procedures for the reconciliation and reporting of locally held funds and require formal supervisory review of the reconciliation and relate "Report of Receipts and disbursement of Locally Held Funds" prior to submission to the Comptroller.

Findings: ISP did not have adequate internal controls over the reconciliation and reporting of locally held funds. A June 30, 1999 report on the Forfeitures Fund was prepared incorrectly and not adequately reviewed prior to inclusion in the GAAP Reporting Package.

Response: Compliance with all recommendations has been accomplished. Written procedures have been developed for the reconciliation and reporting of locally held funds.

Emergency Purchases

REVIEW: 4118

The Illinois Purchasing Act (30 ILCS 505/1) states, “The principle of competitive bidding and economical procurement practices shall be applicable to all purchases and contracts...” The law also recognizes that there will be emergency situations when it will be impossible to conduct bidding. It provides a general exemption for emergencies “involving public health, public safety, or where immediate expenditure is necessary for repairs to State property in order to protect against further loss of or damage...prevent or minimize serious disruption in State services or to insure the integrity of State records. The Chief procurement officer may promulgate rules extending the circumstances by which a purchasing agency may make ‘quick purchases’, including but not limited to items available at a discount for a limited period of time.”

State agencies are required to file an affidavit with the Auditor General for emergency procurements that are an exception to the competitive bidding requirements per the Illinois Purchasing Act. The affidavit is to set forth the circumstance requiring the emergency purchase. The Commission receives quarterly reports of all emergency purchases from the Office of the Auditor General. The Legislative Audit Commission is directed to review the purchases and to comment on abuses of the exemption.

During FY99, the State Police filed four emergency purchase affidavits for the following items:

- \$28,794 for roof replacement at District 6 Communications Building in Pontiac;
- \$126,359.59 for roof replacement at District 9 Headquarters in Springfield;
- \$72,000 for an emergency generator and electrical upgrade at District 13 Headquarters in DuQuoin; and
- \$32,540 to replace a laser tube to analyze fingerprint evidence.

Headquarters Designations

The State Finance Act requires all State agencies to make semiannual headquarters reports to the Legislative Audit Commission. Each State agency is required to file reports of all of its officers and employees for whom official headquarters have been designated at any location other than that at which their official duties require them to spend the largest part of their working time.

In July 1999, the Department reported that 1,674 employees spend the majority of their work time in locations other than their official headquarters.

